DIALOG(R)File 347:JAPIO

06354720 **Image available**
METHOD FOR SAFELY PRINTING DOCUMENT

PUB. NO.: 11-296327 [JP 11296327 A]
PUBLISHED: October 29, 1999 (19991029)
INVENTOR(s): CHAN DAVID
GUPTA DIPANKAR
VAN WILDER BRUNO EDGARD
APPLICANT(s): HEWLETT PACKARD CO <HP>
APPL. NO.: 11-000899 [JP 99899]
FILED: January 06, 1999 (19990106)
PRIORITY: 98300144 [EP 300144], EP (European Patent Office), January 09, 1998 (19980109)
INTL CLASS: G06F-003/12

ABSTRACT

PROBLEM TO BE SOLVED: To improve safety in security by printing a document only when an intended receiver executes conversation with a printing device in order to take-out the previously presented document and print it.
SOLUTION: A client ciphers the document furthermore before transmitting it to a printing server in order to increase security and the printing device 140 decodes the ciphered document before printing. A document storage device 130 receives a ciphered document file and related user identifying information and stores them. Besides, the device 130 receives a request for transferring the ciphered document file having designated identifying information to a designated position. A server receives a request from a printer 140 as against the specified ciphered document, researches the designated ciphered document and transfers the document which is ciphered in a request printer.

?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－296327

(43)公開日　平成11年(1999)10月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ｄ

審査請求　未請求　請求項の数１　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－899

(22)出願日　平成11年(1999)１月６日

(31)優先権主張番号　９８３００１４４．７

(32)優先日　1998年１月９日

(33)優先権主張国　ヨーロッパ特許庁（ＥＰ）

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
HEWLETT－PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000

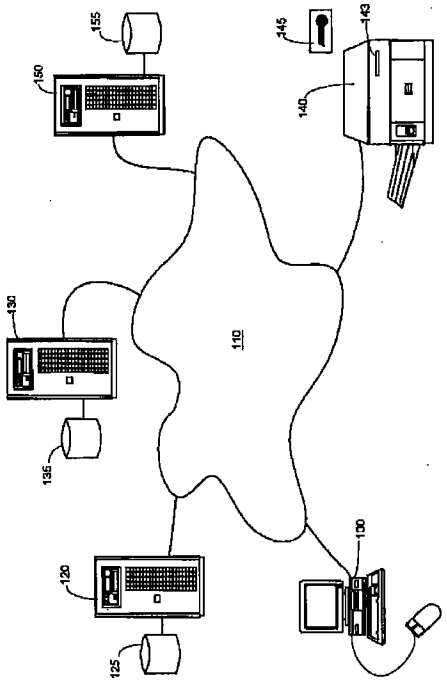
(72)発明者　デビッド・チャン
イギリス、ビーエス９、４エスアール、ブリストル、ヘンリーズ、ウェリントン・ドライブ　14

(74)代理人　弁理士　岡田　次生

最終頁に続く

(54)【発明の名称】　安全にドキュメントを印刷する方法

(57)【要約】
【課題】意図された受け手が印刷装置と対話するときだけ、ドキュメントの印刷が可能になるようにし、セキュリティ上の安全性を向上させる。
【解決手段】送信側が、印刷すべきドキュメントを選択し、ドキュメントの意図された受け手を特定し、意図された受け手のための第1の識別子を伴うドキュメントを、クライアントから印刷サーバに伝送させる。受け手が第2の識別子を印刷装置に提供し、印刷装置が印刷サーバからドキュメントを受け取るため、該第2の識別子を含む要求を印刷サーバに伝送する。印刷サーバが要求を受け取り、前記第2の識別子と格納された第１の識別子とを比較し、一致する識別子については、第1の識別子に関連するドキュメントを印刷装置に転送する。



【特許請求の範囲】
【請求項１】 クライアント、印刷サーバ、印刷装置および分散コンピュータシステムの構成要素を相互接続するためのネットワークを有する分散コンピュータシステムにおいてドキュメントを印刷する方法であって、
送信側が、印刷すべきドキュメントを選択し、ドキュメントの意図された受け手を特定し、意図された受け手のための第1の識別子を伴うドキュメントを、クライアントから印刷サーバに伝送させるステップと、
印刷サーバで前記ドキュメントおよび関連する前記第1の識別子を受け取り、格納するステップと、
受け手が第2の識別子を印刷装置に提供し、該印刷装置が印刷サーバからドキュメントを受け取るため、該第2の識別子を含む要求を印刷サーバに伝送するステップと、
印刷サーバが前記要求を受け取り、前記第2の識別子と格納された第１の識別子とを比較し、一致する識別子については、前記第1の識別子に関連する前記ドキュメントを前記印刷装置に転送するステップと、
前記印刷装置がドキュメントを受け取り、印刷するステップと、を含む印刷方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明はドキュメントのハードコピー生産に関連し、特にドキュメント印刷に関連する。
【０００２】
【従来の技術】例えば、それぞれマイクロソフト(TM)ワードまたはマイクロソフト(TM)パワーポイントのようなコンピュータ・ベースのテキスト編集パッケージまたはグラフィックスパッケージを使用して、ドキュメントをデザインまたは生成することがよく知られている。いったん生成されると、ドキュメントは印刷することができる。典型的には、そのパッケージまたは印刷ドライバーがドキュメントを、プリンタによって受け取られ変換されることができるプリンタ・ファイルにフォーマットする。プリンタ・ファイル・フォーマットの例は、PCLまたはポストスクリプト（PostScript）である。そのパッケージによってプリンタファイルは直接プリンタに送られ印刷されるか、後に印刷するために記憶されることができる。
【０００３】この原理は、例えば、レーザープリンタ、インクジェットプリンタ、インパクト式プリンタおよび感熱式プリンタなどの典型的にすべてのタイプのプリンタに適用され、一般的にはプロッタやファクシミリ・マシンなどの他のハードコピー装置にも適用される。便利なことに、プリンタという用語は、そのようなすべての異なったタイプのプリンタその他のハードコピーまたはドキュメントを生成する装置を含む。
【０００４】また、説明の便宜上、「ドキュメント」という用語は、コンピュータ・ディスプレイ上で見られるとき、印刷用に作られたプリンタファイルとしてフォーマットされているとき、およびハードコピーの形であるときを含め、あらゆる状態のドキュメントを示すのに使用される。ドキュメントが記述の任意の位置にある状態は、コンテキストに依存する。また、「ドキュメント」はテキスト、 グラフィックスまたはこれが混在する表現を含んでもよい。
【０００５】分散形計算機システムの到来は、単一の「ネットワーク」プリンタが複数のユーザによって使用されることを可能にした。典型的に、ネットワーク・プリンタは印刷サーバとして分散処理システムの中で作動する計算プラットホームに取り付けられる。代わりに、適当なインターフェイスを与えられると、直接分散処理システムのネットワークに接続するようにすることができるプリンタもある。
【０００６】ネットワーク・プリンタは、ネットワークに直接接続されようと印刷サーバを介して接続されようと、各ユーザは自身のコンピュータ・システムに接続されるか近くに配置されたそれ自身のプリンタを持つ必要がないので、かなりの費用的利点を提供することができる。
【０００７】ネットワーク・プリンタその他の装置にローカル・コンピュータからアクセスする能力は、ユニックス(Unix)、またはマイクロソフト(商標)ウィンドウズ(商標)NTなどのオペレーティングシステムによって容易にサポートされる。これらのオペレーティングシステムは、リモート印刷やデーター管理などのような分散オペレーションを管理するよう設定することができるよう設計されている。
【０００８】
【発明が解決しようとする課題】遠隔ネットワークプリンタ上でドキュメントを印刷する1つの問題は、意図された受け手がドキュメントを取る前に、プリンタに近い任意の人が、自身のものでない機密情報を含む印刷ドキュメントを取り去ったり読んだりすることができることである。これを避ける1つの方法は、機密のドキュメントを印刷する必要があるユーザが、ドキュメントの印刷中、信頼できる人をプリンタのそばに立たせ、印刷するとすぐにドキュメントを集めるようにすることである。これはもちろん不便である。
【０００９】セキュリティを増加させる別の方法は、ローカルプリンタ装置だけに機密の書類を印刷することである。しかしながら、後者の場合は、特に多くのユーザが機密のドキュメントを印刷する必要があるならば、中央に位置するネットワーク・プリンタを持つことの費用的利点が害される。
【００１０】機密ドキュメントのリモート印刷に関連する別の問題は、悪意のある者がローカル・コンピュータとネットワーク・プリンタの間でのデータの転送をイン

ターセプト（傍受）またはモニタすることができることである。例えば、印刷のためにドキュメントを受け取り中のプリントスプーラまたは印刷サーバをアクセスすることができる者はだれでも、ドキュメントをアクセスすることができる。これは非常に望ましくなく、元となるコンピュータに直接付属するローカルプリンタ装置を代わりに使用することによって克服することができる。

【００１１】

【課題を解決するための手段】この発明は、一面においてリモート印刷のセキュリティを増加させることを目指す。

【００１２】第1の面によるとこの発明は、クライアント、印刷サーバ、印刷装置、および分散コンピュータシステムの成分を相互接続するためのネットワークを含む分散コンピュータシステムでドキュメントを印刷する方法を提供する。

【００１３】この方法は、以下のステップを含む。送信側が、印刷すべきドキュメントを選択し、ドキュメントの意図された受け手を特定し、意図された受け手のための第1の識別子を伴うドキュメントを、クライアントから印刷サーバに伝送させるステップ、印刷サーバで前記ドキュメントおよび関連する前記第1の識別子を受け取り、格納するステップ、受け手が第2の識別子を印刷装置に提供し、該印刷装置が印刷サーバからドキュメントを受け取るため、該第2の識別子を含む要求を印刷サーバに伝送するステップ、印刷サーバが前記要求を受け取り、前記第2の識別子と格納された第１の識別子とを比較し、一致する識別子については、前記第1の識別子に関連する前記ドキュメントを前記印刷装置に転送するステップ、および前記印刷装置がドキュメントを受け取り、印刷するステップ。

【００１４】意図された受け手が先に提出されたドキュメントを取り出し印刷するために印刷装置と対話するときだけ、ドキュメントが印刷されるのが好ましい。事実、意図された受け手は送信側と同じ人であってもよい。

【００１５】好ましい実施例では、セキュリティを増加させるためにクライアントは、印刷サーバに伝送する前にさらにドキュメントを暗号化し、印刷装置は暗号化ドキュメントを印刷前に解読する。

【００１６】したがって、ドキュメントがクライアントと印刷装置の間の転送中にインターセプトされたとしても、インタセプトした者がドキュメントを解読するのは簡単ではないであろう。印刷装置がスマートカードと対話し、受け手によって提供されたスマートカードに含まれる情報を使ってドキュメントを取り出し解読するのが好ましい。スマートカードは第２の識別子を含んでいてもよく、ドキュメント復号化（解読）を助けるようにプログラムされていてもよい。

【００１７】第２の面によると、この発明はドキュメントを受け取り印刷するようにされた印刷装置を提供する。

【００１８】この印刷装置は、次の要素を含む。印刷サーバにプリンタを接続するためのインターフェイス;ユーザと対話しユーザから識別情報（identity: アイデンティティ）を受け取るための入出力手段；ユーザの識別情報を含む、ドキュメントを求める要求を生成し、該要求を印刷サーバに伝送し、印刷サーバからドキュメントを受け取るための処理手段；およびユーザのためにドキュメントを印刷するための手段。

【００１９】この発明の他の面、特徴および実施例は、後続の詳細な説明および請求項から当業者に明らかになるであろう。

【００２０】

【発明の実施の形態】この発明の実施例を図面を参照して説明する。図1において、ローカル・コンピュータ100、例えばウィンドウズ NT 4.0の下で作動するインテルのペンティアム（Pentium）ベースのコンピュータは、キーボード、ディスプレイおよびマウス（図示せず）などの標準的な構成要素を含む。ローカル・コンピュータ100は、例えばTCP/IPプロトコルをサポートするネットワークであるネットワーク110に取り付けられる。ローカル・コンピュータ100は、安全な印刷が必要なときユーザによって開始することができるソフトウェア・ルーチンである安全なプリンタ・プロセスまたはクライアントを提供する。このプロセスおよびこの実施例における他のすべてのプロセスは、C++のような任意の汎用プログラミング言語で書くことができる。

【００２１】ディレクトリ・サーバ120、ドキュメント記憶装置130、安全なプリンタ140、および課金エンジン150もまたネットワーク110に接続されている。

【００２２】ディレクトリ・サーバ120は、ユーザ・プロファイルとして知られるユーザ特定情報のデータベース125にアクセスするコンピュータ上で走るプロセスである。ディレクトリ・サーバ120は、要求発行プロセスから特定ユーザの特定情報に対する要求を受け取り、可能なときはいつも要求発行プロセスに特定の情報を返すようになっている。ディレクトリ・サーバ120を走らせるコンピュータは、適切なインターフェイスを通してネットワーク100に接続されたユニックスまたはウィンドウズNTプラットホームであってよい。

【００２３】この実施例におけるディレクトリ・サーバ120は、問合わせを受け取り関連データを返す単純なデータベースであるが、ノベルのNDSまたはマイクロソフトのアクティブ・ディレクトリ（Active Directory）などのような特注のディレクトリ・サービスをベースとするものでもよい。この実施例に従ってディレクトリ・サーバ120は、ユーザ識別情報を含む要求を受け取り特定されたユーザに関連する公開の暗号化キーを少なくとも返すように設定されている。ディレクトリ・サーバ120

との通信は、軽量ディレクトリ・アクセス・プロトコル(LDAP：Lightweight Directory Access Protocol)などのようなネットワーク・プロトコルとなされる。

【００２４】ドキュメント記憶装置130は、暗号化されたドキュメント・ファイルおよび関連するユーザ識別情報を受け取り格納するコンピュータ上で走るプロセスである。また、ドキュメント記憶装置130は、指定された識別情報を持つ暗号化されたドキュメント・ファイルを指定された位置に転送するための要求を受け取る。また、ディレクトリ・サーバ120を走らせるコンピュータは、適切なインターフェイスを通してネットワーク100に接続されたユニックスまたはウィンドウズNTプラットホームであってよい。

【００２５】実際上、ドキュメント記憶装置130は、例えばディスクドライブ135によって提供されるような大きなデータ記憶装置にアクセスする変更されたプリントスプーラまたは印刷サーバ・プロセスであってよい。また、スプーラまたはサーバは、特定の暗号化されたドキュメントに対するプリンタからの要求を受け取り、指定された暗号化されたドキュメントをサーチし、要求プリンタに暗号化されたドキュメントを転送するよう変更されている。

【００２６】この実施例におけるドキュメント記憶装置130は、適切なプロトコルを使用してドキュメントを任意の要求プリンタその他の装置に返すよう設定されている点で、分散処理システムの信頼性のない部分である。

【００２７】セキュリティがさらに重要である他の実施例では、ドキュメント記憶装置130はさらに認証の機能性を組み込み、それによってドキュメント記憶装置が要求プリンタまたはスマートカード・ユーザを認承することを可能にする。例えばディジタル署名を使用する認証システムはよく知られているので、ここではこれ以上詳細に触れない。

【００２８】この実施例によるプリンタ140のアーキテクチャが図２に詳しく示されている。図2は印刷エンジン210を制御する中央処理装置(CPU)200について図示する。印刷エンジン210は、印刷を行う任意のプリンタの標準の部分であり、詳細はここでの記述の範囲を超えている。読み取り専用メモリ(ROM)220は適切なシステムバス205によってCPU200に接続されている。ROM220はプリンタのための制御プログラムを形成する命令を含んでいる。不揮発性のメモリ(NV-RAM)230およびメインメモリ(DRAM)240がまた、システムバス205に接続されている。

【００２９】NV-RAM230は、プリンタにダウンロードされたサービスを受け取り格納するためのEEPROMまたはフラッシュRAMであってよい。DRAM240は、プリンタによって印刷すべきジョブを受け取るためのバッファ・メモリとして使用され、この実施例ではまた、CPU200によって、復号化のための作業スペースとしておよびセッション・キーの記憶装置として使用される。

【００３０】これまで記述したプリンタ140のすべての機能は、多くの一般に利用可能なプリンタに関して標準的なものである。また、 図は、すべてシステムバス205を通してCPUに接続したネットワークインターフェイス250、たとえば「ペーパアウト」など様々なセンサ260、フロントパネル・ディスプレイおよびキーパッド270といった標準的なプリンタ機能を図示する。

【００３１】スマートカード読取装置280がシステムバス205に接続されているが、これは、プリンタにRS232ポートがある場合はこれを介して接続することもできる。このように、プリンタの有意な標準的でないハードウェア機能は、スマートカード読取装置280だけである。他の違いはソフトウェアまたはファームウェア処理に依存する。

【００３２】スマートカード読取装置は一般的に入手可能であり受け入れられた標準に従う。この実施例で使用されるスマートカード読取装置は、ISO7816標準(レベル1～4)および国際標準規格に含まれないいくつかの機能性を支援する。対応するスマートカードも容易に入手でき、ここで記述されるように作動するようプログラムすることができる。

【００３３】実際上、スマートカード読取装置は標準的なプリンタのケーシングに組み込むことができる。このように、この場合、プリンタに関するめぼしい違いは、スマートカード145が挿入されて検索されることができるケーシングのスロット143だけである。

【００３４】図2に示した機能を一般的に持つプリンタは、ヒューレット・パッカード・レーザジェット５（LaserJet 5）またはヒューレット・パッカード・レーザジェット4000（LaserJet 4000）である。どちらのプリンタにおいても、プリンタの従来の制御プログラムは、プリンタのROM220中のファームウェアを取り替えるか、プリンタのフラッシュメモリNV-RAM230にネットワークからダウンロードすることができる「サービス」を創ることによって、ここで説明したように変更することができる。

【００３５】ヒューレット・パッカードその他のプリンタにおいて制御プログラムを変更する方法に関する詳細は、ここでの説明の範囲を超えているが、ヒューレット・パッカード・カンパニーまたは他のそれぞれのプリンタ・メーカーから容易に入手することができる。

【００３６】プリンタ自体は暗号化ドキュメントを取り出し処理する機能性を持つようプログラムされた、一体的なスマートカード読取装置を備えたプリンタを以上に説明した。代替の実施例では、汎用プリンタおよびシリアルポートを通してプリンタに接続された外部のスマートカード・リーダユニットからなる印刷装置が用いられてもよい。スマートカード・ユニットにはネットワークにユニットを接続するためのネットワークインターフェイス、ならびに汎用プリンタとスマートカード・リーダ

ユニットの組み合わせがこの発明による印刷装置として作動するよう適切にプログラムされたプロセッサおよびメモリが備えられている。

【００３７】事実上、スマートカード・リーダユニットは、自身のスマートカードを挿入する受け手と対話し、セッションキーおよび暗号化されたドキュメントを検索し解読するためドキュメント記憶装置130と対話し、ドキュメントを印刷すべきプリンタに転送するよう設計されている。

【００３８】明らかに、この実施例は、暗号化されていないドキュメントをスマートカード・リーダユニットとプリンタの間の通信リンク上でパスすることによって、総合的なシステムのセキュリティに弱いリンクを提供する。しかしながら、プリンタとスマートカード・リーダユニットが共同で配置されるとき、関連するリスクは最小になると考えられる。

【００３９】既存の印刷装置を使用して費用効率がよい方法でこの発明を利用しようとする場合、そのような装置が好ましいかもしれない。プリンタとスマートカード・リーダユニットにおけるこの発明を実行するために必要な機能性は、情況に依存して他の方法で仕切られてもよいと考えられる。

【００４０】課金システム150はコンピュータで走るプロセスであり、安全な印刷システムのユーザに電子的に課金する。ユーザが課金される3つのメイン領域があり、それらは、暗号化されたドキュメントのドキュメント記憶装置130への提出、ドキュメント記憶装置130によるドキュメントの指定期間内の格納、およびドキュメントの成功裏の印刷である。ディレクトリ・サーバ120の使用など他のことも潜在的に課金されうる。送信側か受け手またはその両者がこれらの動作のいずれかに対して課金されうる。例えば、送信側が提出のために課金されてもよく、受け手がドキュメントの記憶と印刷に対して課金されてもよい。もちろん、送信側と受け手は同じ人であってもよく、同じ組織の異なった人々であってもよく、この場合、一人の人か一つの組織がすべてについて課金される。

【００４１】さらに、ドキュメント記憶装置の所有者およびプリンタの所有者は、異なった独立のサービス・プロバイダーであってもよい。例えば、プリンタが公共の場所にあり、公共による使用のためのものである場合、プリンタの所有者はサービスの提供に対して財政的な報酬を欲するであろう。したがって、課金システム150がプリンタの所有者に課金された資金を割り当てることができる程度に、プリンタがそれ自身を詳細に特定することが必要であろう。

【００４２】あらゆる行為について、課金される者および支払われる者を特定することが必要である。電子課金の目的のために電子的識別および認証は、電子商取引のフィールドでよく知られているので、ここでは詳細を記述しない。

【００４３】安全な印刷ジョブを提出する際のローカル・コンピュータ100のオペレーションを図3のフローチャートを参照して説明する。

【００４４】図3のステップ300で、ローカル・コンピュータのオペレータ(図示せず)、すなわちドキュメントの送信側は、印刷のために提出される、例えばワープロ処理されたドキュメントのようなドキュメントを持っている。送信側はステップ305でドキュメントの安全な印刷のために安全な印刷プロセスを開始する。ステップ310で安全な印刷プロセスは、グラフィカル・ユーザー・インターフェイスを生成する。このインターフェイスは、送信側にドキュメントの詳細および意図された受け手の識別情報を入力することを要求する。意図された受け手はもちろん、送信側自身かもしれない。送信側はステップ315に必要な詳細を入れる。送信側から有効な入力を受け取ると、ステップ320でプロセスは、送信側によって入力された詳細を含む要求をディレクトリ・サーバ120に送信する。応答してディレクトリ・サーバ120は、ステップ325で安全な印刷プロセスに意図された受け手の公開キーを返す。

【００４５】次にステップ330で、安全なプリンタ・プロセスはドキュメントをプリンタによって解明できるPostScriptやPCLのようなページ記述言語にフォーマットする。明らかに、言語はプリンタのタイプまたは他の使用されるべきハードコピー装置に依存する。安全なプリンタ・プロセスは、ステップ335でその完全性を保ちながら大量の暗号化をフォーマットされたドキュメントに適用する。安全なハッシュ・アルゴリズム（Secure Hash Algorithm：SHA-1)および対称ブロックまたはストリーム暗号、例えばデータ暗号規格（Data Encryption Standard：DES)のようなメッセージダイジェスト関数を使用してこれを達成することができる。暗号は暗号化のために安全なプリンタ・プロセスによって発生される乱数を使用する。乱数はセッション・キーを構成する。このステップは、対称的な暗号化ステップであり、ドキュメントを解読するためにセッション・キーにアクセスする受け手に依存する。

【００４６】MD5のような代替のメッセージ・ダイジェスト・アルゴリズム、CASTやIDEAなどの対称的な暗号、およびだ円曲線ElGamal暗号化法のような非対称のアルゴリズムを、先に指定したアルゴリズムの代わりに使用することができる。

【００４７】ステップ340で安全なプリンタ・プロセスは、意図された受け手の取り出された公開キーを使用して、RSAのような非対称の暗号化アルゴリズムをセッション・キーに適用する。このように、このステップの後は、公開キーに関連する個人的（プライベート）キーの知識を持っている者だけが、セッション・キーを解読し、したがってドキュメントを解読することができる。

【００４８】全体のプロシージャが比較的信頼された安全な環境の境界の中で制定されるいくつかの実施例では、暗号化段階を使用する必要はないと感じられるかもしれない。そのような場合、例えばメッセージが一つのビルの外部に決して伝送されない場合、受け手がプリンタにいるときだけドキュメントが印刷されるようにすれば十分であろう。

【００４９】ステップ345で安全な印刷プロセスは、ネットワーク110の向こう側のドキュメント記憶装置130に、暗号化されたドキュメントを含むメッセージ、ドキュメントのための「封筒」（暗号化されたセッション・キーが入っている）、および意図された受け手のそれぞれの識別情報を転送する。

【００５０】最後にステップ350において、ドキュメント記憶装置130はメッセージを受け取り、適切にそれをハードディスク135に格納する。

【００５１】ドキュメント記憶装置130から検索されたドキュメントを安全に印刷するプロセスを図4のフローチャートを参照して説明する。

【００５２】図4のステップ400で、ドキュメント記憶装置130に格納されているドキュメントの意図された受け手は、彼のスマートカードを安全なプリンタ140のスマートカード読取装置（リーダ）280に挿入する。スマートカードは受け手の識別情報および受け手の個人的キーを含んでいる。フローチャートでは図示されないが、受け手がスマートカードの真正な所有者であり、それを見つけたり盗んだ者ではないことを確かめるために、プリンタが受け手に個人識別番号の入力を要求するのが、この段階では典型的である。

【００５３】スマートカード読取装置280はステップ405でスマートカードを読取り、そこから識別情報を抽出する。次いでステップ410で、スマートカード読取装置280は識別情報をプリンタのCPU200に転送する。CPU200は識別情報をステップ415で受け取り、ステップ420で識別情報を含むメッセージを生成し、ステップ425でドキュメント記憶装置130に転送する。

【００５４】ステップ430で、ドキュメント記憶装置130がメッセージを受け取り、ステップ435で同じ識別情報を持つドキュメントを求めてハードディスク135をサーチする。の実施例では、ドキュメント記憶装置130は1つのドキュメントを見つける。しかしながら一般になにもないかもしれないし、ハードディスク135に格納された一致する識別情報を持つ任意の数のドキュメントがあることもある。この段階でドキュメント記憶装置130およびプリンタ140は、状態情報を受け手に提供するために対話するようにされていてもよく、この情報は、プリンタのフロントパネル・ディスプレイ270に表示され、例えば印刷待ちのドキュメントの数とか印刷待ちのドキュメントはないとかを示すことができる。さらに、受け手はどのドキュメントを取り出したいかを選択することさえできる。

【００５５】次にステップ440で、ドキュメント記憶装置130は一致する識別情報を持つドキュメントの封筒だけをプリンタ140に返す。原則的に、この段階でもドキュメントを送ることができるが、そうするかどうかはドキュメントのサイズおよび使用可能なプリンタバッファ・メモリの量による。プリンタ140に全体のドキュメントを受け取ることができるかなりの量のRAM240があるのでなければ、封筒だけを取り出すのがここでは好ましいと信じられる。

【００５６】ステップ445でプリンタは封筒を受け取り、ステップ450で暗号化されたセッション・キーをスマートカード読取装置280に転送する。スマートカード読取装置280は暗号化されたセッション・キーをスマートカードに転送し、スマートカードは続いてステップ455でそこに格納された個人的キーを使用してセッション・キーを解読する。スマートカードはステップ460で解読セッション・キーを出力し、スマートカード読取装置280はステップ465でセッション・キーをCPU200に転送する。

【００５７】個人的なキーがスマートカードを決して離れる必要がなく、したがってプリンタからさえ秘密のままでいられるので、セッション・キーを取り出すためのこの技法は極めて有利である。

【００５８】プリンタ140はステップ470でメッセージをドキュメント記憶装置130に転送し、ドキュメント記憶装置は暗号化されたドキュメントをプリンタ140に伝送する。ステップ475でドキュメント記憶装置130がメッセージを受け取り、ステップ480でドキュメントをプリンタ140に伝送する。ステップ485でプリンタ140はドキュメントを受け取り、ステップ490でセッション・キーを使用してそれをページ記述言語に解読変換する。

【００５９】最後にステップ495でプリンタは意図された受け手のためのドキュメントを印刷する。代わりに、ドキュメントの復号化を行うようにスマートカード自体がプログラムされていてもよいと考えられる。これはもちろん設計上の決定である。

【００６０】ネットワーク110は、ローカルエリアネットワーク、広域ネットワークまたはグローバル領域のネットワークであってもよい。例えば、グローバル領域ネットワークの場合にローカル・コンピュータ100はロンドンのオフィスに位置することができ、プリンタは東京かニューヨークの空港に位置することができる。同様に、ディレクトリ・サーバ120およびドキュメント記憶装置130は、世界のどこでも位置することができる。

【００６１】いくつかの実施例では応答性目的のために、インターネット・ミラーサイトと同様のミラー・ドキュメント記憶装置(図示せず)を持つことが望ましい。ミラー記憶装置では、1つの記憶装置のデータが他の地理的に遠方のドキュメント記憶装置にコピーされる。こ

のように、例えばロンドン・ベースのデータ・サーバ、および東京、ニューヨーク・ベースのデータ・サーバがありうる。ドキュメントを受け取ると、ロンドンのデータ・サーバはドキュメントを東京とニューヨークのデータ・サーバの両方にコピーするので、受け手は使用されるプリンタに最も近いデータ・サーバからドキュメントを取り出し印刷することができる。

【００６２】明らかに、受け手が、ドキュメントを印刷したいときに、最も居そうなところが知られていれば、データ・ミラーリングを調整することができる。例えば、受け手がニューヨークに居そうであるが、そうではなくロンドンに居るかもしれないならば、ロンドンで提出されるドキュメントをニューヨーク・ベースのデータ・サーバにミラーさせればよい。そのような受け手位置の情報は、ディレクトリ・サーバ120によって格納されたユーザプロファイル情報の一部を形成することができる。このように、これらの情況の下における位置の情報は、公開キー情報と共にローカル・コンピュータ100に返され、また、この情報はドキュメント記憶装置130に転送される。

【００６３】ディレクトリ・サーバ120は他のユーザプロファイル情報を保持すると考えられる。例えば、受け手は、1台の指定されたプリンタからだけドキュメントを受け取ることを願うことがある。この場合、ディレクトリ・サーバ120によって返された情報がこのことを反映し、ドキュメント記憶装置130は、暗号化されたドキュメントを指定されたプリンタにだけ送る。ディレクトリ・サーバ120によって特定のユーザのために保持される他の情報がプリンタ情報を含むことがあり、そのプリンタ情報は、ドキュメントがローカル・コンピュータ100によってどのようにフォーマットされるか、例えばPostScriptまたはPCLのどちらにドキュメントをフォーマットするかを決定するものであることがある。一般に、ユーザは、例えばインターネットを通してディレクトリ・サーバ120にアクセスすることができ、必要であるときに自身のユーザプロファイルを変更することができると期待される。

【００６４】上述した構成要素およびプロセスは、異なるコンピュータ上に常駐する必要はないことがわかる。例えば、ローカル・コンピュータ100はディレクトリ・サーバ、ドキュメント記憶プロセス、および安全なプリンタ・プロセスをサポートすることができる。

【００６５】その上、ここで記述されるプロセスのすべてまたはどれかが見つけられなく、分散環境に接続されたたくさんの異なるコンピュータシステムのどれかから呼ぶことができないことになるような理由はない。その上で、安全な印刷を必要とするドキュメントが、暗号化されないで、公開的にアクセス可能なまたは低セキュリティの通信チャネルを通して送られることがないようにすることが重要である。

【００６６】この発明は、例として次の実施形態を含む。

【００６７】1. クライアント、 印刷サーバ、 印刷装置および分散コンピュータシステムの構成要素を相互接続するためのネットワークを有する分散コンピュータシステムにおいてドキュメントを印刷する方法であって、送信側が、印刷すべきドキュメントを選択し、ドキュメントの意図された受け手を特定し、意図された受け手のための第1の識別子を伴うドキュメントを、クライアントから印刷サーバに伝送させるステップと、印刷サーバで前記ドキュメントおよび関連する前記第1の識別子を受け取り、格納するステップと、受け手が第2の識別子を印刷装置に提供し、該印刷装置が印刷サーバからドキュメントを受け取るため、該第2の識別子を含む要求を印刷サーバに伝送するステップと、印刷サーバが前記要求を受け取り、前記第2の識別子と格納された第１の識別子とを比較し、一致する識別子については、前記第1の識別子に関連する前記ドキュメントを前記印刷装置に転送するステップと、前記印刷装置がドキュメントを受け取り、印刷するステップと、を含む印刷方法。

【００６８】2.　上記1による方法であって、クライアントが印刷サーバに伝送する前にドキュメントを暗号化し、印刷装置が暗号化されたドキュメントを印刷前に解読する印刷方法。

【００６９】3.　上記2による方法であって、受け手は暗号化されたドキュメントを解読するのに必要な手段を印刷装置に提供する印刷方法。

【００７０】4.　上記3による方法であって、印刷装置は、情報および/または受け手によって提供されたスマートカードにプログラムされた機能性を使用して、ドキュメントを取り出し、解読するためにスマートカードと対話する。

【００７１】5.　上記4による方法であって、受け手によって提供されたスマートカードが第2の識別子を含むデータを格納し、印刷装置が第2の識別子をスマートカードから抽出する印刷方法。

【００７２】6.　上記4または5による方法であって、復号化アルゴリズムでプログラムされ秘密を格納するスマートカードが印刷装置から暗号化された情報を受け取り、秘密を使用して暗号化された情報を解読し、解読情報を印刷装置に返すようにした印刷方法。

【００７３】7.　上記6による方法であって、クライアントを含み、対称的な暗号化アルゴリズムのキーである第1のキーを使用してドキュメントを暗号化し、非対称の暗号化アルゴリズムの公開キーである第2のキーを使用して第1の暗号化キーを暗号化し、暗号化されたドキュメントおよび関連する暗号化された第1のキーを伴う第１の識別子を印刷サーバに伝送するようにした印刷方法。

【００７４】8.　上記6による方法であって、意図され

た受け手の識別情報に基づいて、クライアントが第2のキーをキーの貯蔵庫から入手するようにした印刷方法。

【００７５】9.　上記7または8による方法であって、印刷装置を含み、要求に応答して印刷サーバから暗号化された第1のキーを受け取るステップと、暗号化された第１のキーをスマートカードに転送し、非対称の暗号化アルゴリズムの個人的なキーである秘密を使用してスマートカードが暗号化された第1のキーを解読し、第1のキーを印刷装置に返すステップと、暗号化されたドキュメントを解読するために第1のキーを使用するステップとを含む印刷方法。

【００７６】10.　上記の任意の1つの方法による動作をするように構成された印刷装置。

【００７７】11.　上記1～9の任意の1つの方法による動作をするよう構成されたクライアント。

【００７８】12.　上記1～9の任意の1つの方法による動作をするよう構成された印刷サーバ。

【００７９】13.　上記1～9の任意の1つの方法による動作をするよう構成された分散形計算方式システム。

【００８０】14.　ドキュメントを受け取り印刷するようにされた印刷装置であって、印刷サーバにプリンタを接続するためのインターフェイスと、ユーザと対話しユーザから識別情報を受け取るための入出力手段と、ドキュメントを求めるユーザの識別情報を含む要求を発生し、要求を印刷サーバに伝送し、印刷サーバからドキュメントを受け取るための処理手段と、ユーザのためにドキュメントを印刷するための手段と、を有する印刷装置。

【００８１】15.　上記14による印刷装置であって、印刷サーバから受け取られた暗号化されたドキュメントを受け取り解読するための処理手段を備える印刷装置。

【００８２】16.　上記15による印刷装置であって、入出力手段は、ユーザから暗号化されたドキュメントを解読するために必要な手段を提供する脱着可能な処理手段を受け取るようになっている印刷装置。

【００８３】17.　上記16による印刷装置であって、入出力手段はユーザからスマートカードを受け取るためのスマートカード読み取り装置を含む印刷装置。

【００８４】18.　上記17による印刷装置であって、スマートカード読み取り装置は、スマートカードからユーザの識別情報を抽出するようになっている印刷装置。

【００８５】19.　上記17による印刷装置であって、スマートカード読み取り装置は、暗号化された情報をスマートカードに転送し、スマートカードから暗号化されていない情報を受け取るようになっており、スマートカードは暗号化された情報を受け取り、スマートカードに格納された秘密を使用して暗号化された情報を解読し、解読情報を返すようになっている印刷装置。

【００８６】20.　上記19による印刷装置であって、要求に応答し印刷サーバから暗号化された第1ののキーを受け取るための手段と、スマートカードが秘密を使用して暗号化された第1のキーを解読し第１のキーを返すように、暗号化された第1のキーをスマートカードに転送するための手段と、第１のキーを使用して暗号化されたドキュメントを解読するための手段と、を備える印刷装置。

【００８７】21.　上記17～20の任意の1つによる印刷装置であって、一体的スマートカード読取装置を含めて印刷装置の構成要素を含むように構成されたケーシングであって、スマートカードをケーシングを通してスマートカード読取装置に受け取るためのスロットを有するケーシングを備えた印刷装置。

【００８８】22.　上記17～20の任意の1つによる印刷装置であって、インターフェイス手段およびインターフェイス手段を通してプリンタと接続するスマートカード読み取り装置を有するプリンタを備えた印刷装置。

【００８９】23.　上記22による印刷装置であって、スマートカード読み取り装置がネットワークに該装置を接続するためのインターフェイス手段を有する印刷装置。

【００９０】24.　上記23による印刷装置であって、上記スマートカード読み取り装置は、スマートカードからユーザ識別情報を抽出するための手段と、要求を発生しネットワークを通して印刷サーバに伝送するための手段と、印刷サーバから暗号化されたドキュメントおよび暗号化されたキーを受け取るための手段と、スマートカードがキーを解読し返すように、暗号化されたキーをスマートカードに転送する手段と、キーを使用して、暗号化されたドキュメントを解読する手段と、印刷すべきプリンタにドキュメントを転送する手段と、を備える印刷装置。

【００９１】25.　上記22～24の任意の1つによる印刷装置で動作するよう構成されたスマートカード読み取り装置。

【００９２】

【発明の効果】この発明によると、ドキュメントを安全に印刷することができる。

【図面の簡単な説明】

【図１】この発明の実施例に従って安全な印刷を支援する分散コンピューティング環境について図示する図。

【図2】この実施例によるプリンタのためのアーキテクチャのブロック図。

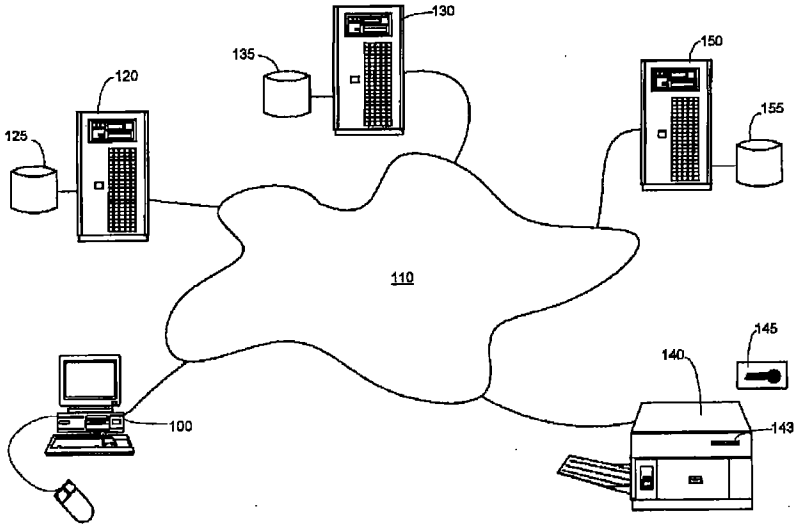
【図３】ユーザが安全な印刷のためにドキュメントを提出するステップについて図示するフローチャート。

【図４】印刷ジョブの安全な取り出しおよび印刷に含まれるステップについて図示するフローチャート。

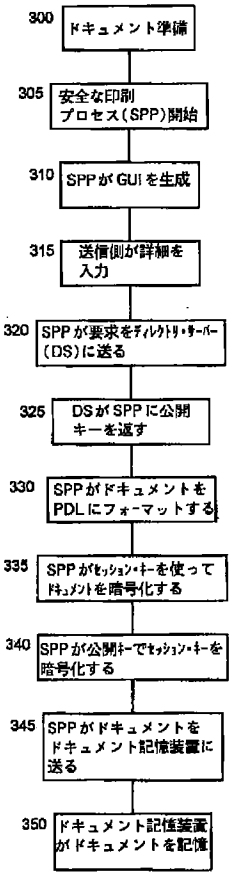
【符号の説明】

１００：　ローカル・コンピュータ（クライアント）
１１０：　ネットワーク
１３０：　ドキュメント記憶装置（印刷サーバ）
１４０：　プリンタ

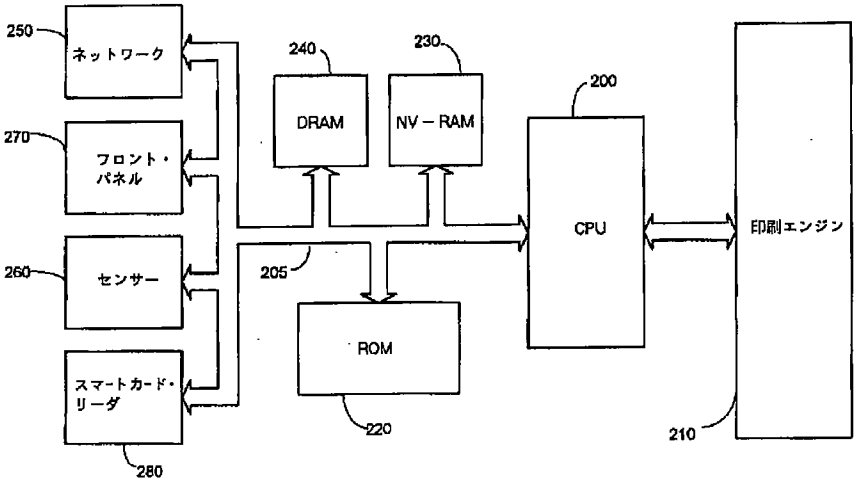
【図１】


130
135
150
120
155
125
110
145
140
100
143

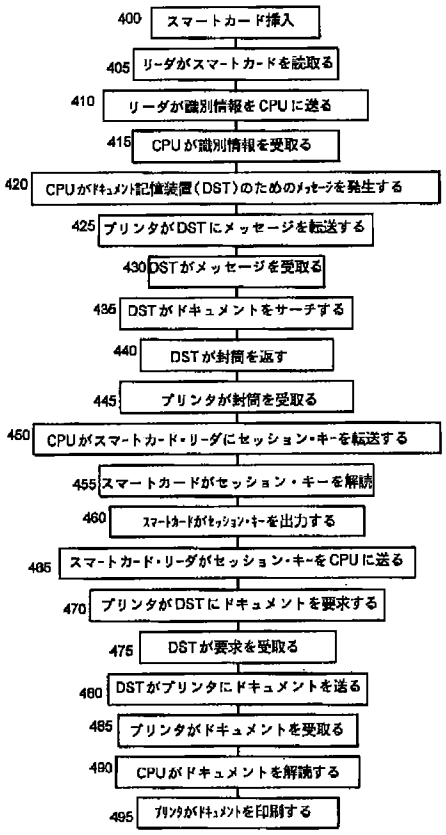
【図３】


300
ドキュメント準備
305
安全な印刷プロセス(SPP)開始
310
SPPがGUIを生成
315
送信側が詳細を入力
320
SPPが要求をディレクトリ・サーバー(DS)に送る
325
DSがSPPに公開キーを返す
330
SPPがドキュメントをPDLにフォーマットする
335
SPPがセッション・キーを使ってドキュメントを暗号化する
340
SPPが公開キーでセッション・キーを暗号化する
345
SPPがドキュメントをドキュメント記憶装置に送る
350
ドキュメント記憶装置がドキュメントを記憶

【図２】


250
ネットワーク
240
DRAM
230
NV－RAM
200
270
フロント・パネル
CPU
印刷エンジン
260
センサー
205
ROM
スマートカード・リーダ
220
210
280

【図4】



フロントページの続き

(72)発明者　ディパンカー・グプタ
アメリカ合衆国94086カリフォルニア州サニーベイル、イースト・イブリン・アベニュー　825、アパートメント　428

(72)発明者　ブルーノ・エドガード・ヴァン・ワイルダー
イギリス、ビーエス8、2ビーゼット、ブリストル、クリフトン、アルマ・ロード　27